View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Modeling Online Passwords Protection Intention

Lixuan Zhang
Augusta State University

William McDowell
Augusta State University

Follow this and additional works at: http://aisel.aisnet.org/amcis2009

Recommended Citation
Zhang, Lixuan and McDowell, William, "Modeling Online Passwords Protection Intention" (2009). *AMCIS 2009 Proceedings*. 339.
http://aisel.aisnet.org/amcis2009/339

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Modeling Online Passwords Protection Intention

ABSTRACT

Using the Protection Motivation Theory, the paper tests a model password protection intention of online users. Hypotheses are proposed concerning the intention to engage in good password practice. Data were collected from 182 college students who use the Internet. The result suggests that fear, response cost and response efficacy are significantly related to online password protection intention. However, perceived severity and vulnerability are not significant predictors. The study suggests that reducing cognitive costs for passwords is imperative.

Keywords

Password protection, protection motivation theory, privacy, security

INTRODUCTION

The growth of ecommerce and the Internet has increased the number of passwords for each online user. Password is one of the most common mechanisms that users employ to protect their online privacy and security. A large-scale study of web passwords involving half a million users shows that each user has about 25 accounts that require passwords and a user types eight passwords per day on average. (Florêncio and Herley, 2007). Authenticating a person's identity, passwords serve the first line of defense mechanism to prevent malicious hackers. Passwords are employed to protect users' online information including financial information, personal emails and various website accounts. However, researchers find that passwords are one of the most likely human error risk factors to impact information systems (Carsten, McCauley-Bell, and DeMara, 2004). Passwords are very vulnerable to hackers' attack. In a study examining the vulnerability of online passwords, more than half of the passwords for 516 users on an ecommerce website were cracked in less than 4 hours and almost a third of these passwords were cracked in one minute (Cazier and Medlin, 2006).

Given the popular usage of passwords as well as their vulnerability, companies and website vendors often offer guidance to users on how to create strong passwords. For example, Google offers tips for creating a secure password and provides a password strength meter, which assesses passwords as weak, fair, good or strong based on the password length, character composition and filtering of weak choices (such as the word "password"). A weak password is not allowed to be used. Similarly, Microsoft allows a system administrator to set a stringent password policy enforcing password aging, minimum length or a mix of letters, numbers and symbols. However, a recent study finds that the enforced password composition rules do not discourage users from using meaningful information in their passwords (Campell, Kleeman and Ma, 2007). Users still choose meaningful or a combination of meaningful information to create their passwords. The enforcement of composition rules is not effective in changing the users' password behavior.

The ineffective enforcement of composition rules of passwords reveals that users are not highly motivated to use strong passwords. However, little research has examined the protection motivations of the strong password usages. Previous research has examined users' password management strategies (Gaw and Felten, 2006), user behavior associated with password security (Bryant and Campbell, 2006) and the core characteristics of user-generated passwords (Zviran and Haga, 1999). Although these studies provide rich insights on users' passwords behavior, most of them are descriptive studies and lack a sound theoretical background. Using the protection motivation theory, this paper intends to investigate the protection motivations of the online users associated with their passwords behavior.

The rest of the paper is organized as follows. The study reviews related literature about passwords usage followed by a description of protection motivation theory. Then hypotheses about the protection motivation for using passwords are formulated. Data are analyzed and results are discussed. Finally, implications of the research are presented along with implications for practice and for future research.

LITERATURE REVIEW

Passwords are used widely as an authentication method. Compared to their alternatives including hardware authentication and biometric identifications, passwords are simple to use and do not have huge financial costs involved. However, online

users often regard password usage as nuisance rather than protection (Adams and Sasse, 1999). Passwords create an overhead cost for them, whose primary task is to use websites to do their tasks on hands (Weirich and Sasse, 2001) Therefore, online users often choose weak passwords. The following section reviews previous research regarding the length, the composition, the information contained in the passwords, the update frequency and the reuse frequency of passwords.

Passwords should have at least a minimum of 6 characters. The longer a password, the strong it is. In a study examining 997 computer users conducted in 1999, 47% of the respondents did not have a password with a minimum six characters (Zviran and Haga, 1999). However, recent studies show the improvement in password length of computer users. In a study examining the passwords of an e-commerce website, the mean length of the password is 7.4 characters (Gazier and Medlin, 2006). In another study, only about 18% of 884 undergraduate students have passwords with 6 characters or less on their university web mail accounts (Bryant and Campbell, 2006).

Good passwords should mix letters, numbers and special characters. Such passwords are very difficult to crack. Despite the security that such passwords offer, users still prefer alphabetic characters for their passwords. A study shows that more than 80% of respondents used alphabetic characters for their passwords while only 0.7% used the entire ASCII character set as a basis for their passwords (Zviran and Haga, 1999). A study in 2006 still shows that 58.3% only have alphabetic characters; about a third have letters and numbers and fewer than 2% have special characters (Gazier and Medlin, 2006).

Regarding the information contained in the passwords, personal and meaningful information are contained in majority of the passwords. Since most passwords are generated on the spot, online users often choose the terms that they are familiar with. A study conducted in Britain revealed that people choose personal terms as their passwords such as spouse's name, children's name, birth date or phone numbers. One third of respondents used names of athletes, singers, movie stars or fictional characters. Only ten percent picked intelligible passwords or a random string of letters, numbers and symbols (Andrews, 2005). In another study, 75.5% of respondents use personal information as part of passwords (Tamil, Othman, Abidin, Idris, and Zakaria, 2007).

Another problem with passwords is that after users choose their passwords, they rarely change them. In a study conducted by NTA Monitor in 2002, 67% of users rarely or never change their passwords, and a further 22% admit that they would only change their password if forced to by a web site or IT department (). In one study, among people who change their password, 44% of them only change them less than once a year (Bryant and Campbell, 2006). Users often reuse their passwords in multiple accounts. Reusing a password is similar to revealing a password, which make the accounts with all the same passwords vulnerable (Ives et al., 2004).If users reuse a password across many accounts, a hacker can access many accounts if the password is cracked A study reveals that the users have few unique passwords (median=3 and mean=3.31). Users have more accounts over time, but they do not have more unique passwords (Gaw and Felten, 2006). The study of Florêncio and Herley (2007) shows that the average user has 6.5 passwords and each of them is shared across 3.9 different sites.

Overall, users tend to use short passwords, passwords with only letters and passwords with personal and meaningful information. In addition, they tend not to update their passwords and reuse the same passwords across multiple accounts. Humans' cognitive limitations are the main reason why users have these poor password practices. According to Miller (1956), there is a severe limitation on the amount of information that humans are able to process and remember for a short term. In addition, users have limited cognitive resources. Described as cognitive misers (Fiske and Taylor, 1984), they only spend the efforts necessary to make a satisfactory decision rather than an optimal decision. In the case of password choices, users tend to sacrifice the benefits of strong passwords to conserve cognitive efforts. Users have to be strongly motivated to adopt strong password practice. In the following section, we will examine the factors that may motivate users in the lens of protection motivation theory.

THEORETICAL MODEL AND HYPOTHESIS DEVELOPMENT

Protection motivation theory (PMT) was proposed to explain how people cope with potential threats (Rogers, 1975). The theory has been used widely to explain and predict a variety of protective behaviors, especially health-related behaviors. Based on expectancy-value theory, the theory provides a detailed account of social cognitive process underlying protective behaviors. The theory consists of two processes: the threat-appraisal process and the coping-appraisal process. The threat-appraisal process consists of three factors: perceived severity, perceived vulnerability and fear arousal. The coping-appraisal process evaluates a person's ability to cope with the threat. Factors in the coping-appraisal process are response cost, self-efficacy and response efficacy. In this study, we did not investigate self-efficacy since using strong passwords and updating passwords does not require a lot of technical skills.

The outcome of these processes is a decision to initiate, continue or discontinue a specific behavior. Therefore, measures of behavioral intention are the typical dependent variable in PMT. Two meta analysis of PMT shows that the theory has been

proved useful in predicting health-related intentions (Floyd, Prentice-Dunn and Rogers, 2000; Milne, Paschal and Orbell, 2000) our study. In this study, we will examine how the PMT variables will affect intention of implementing strong password practice. Figure one depicts the theoretical model for the study.

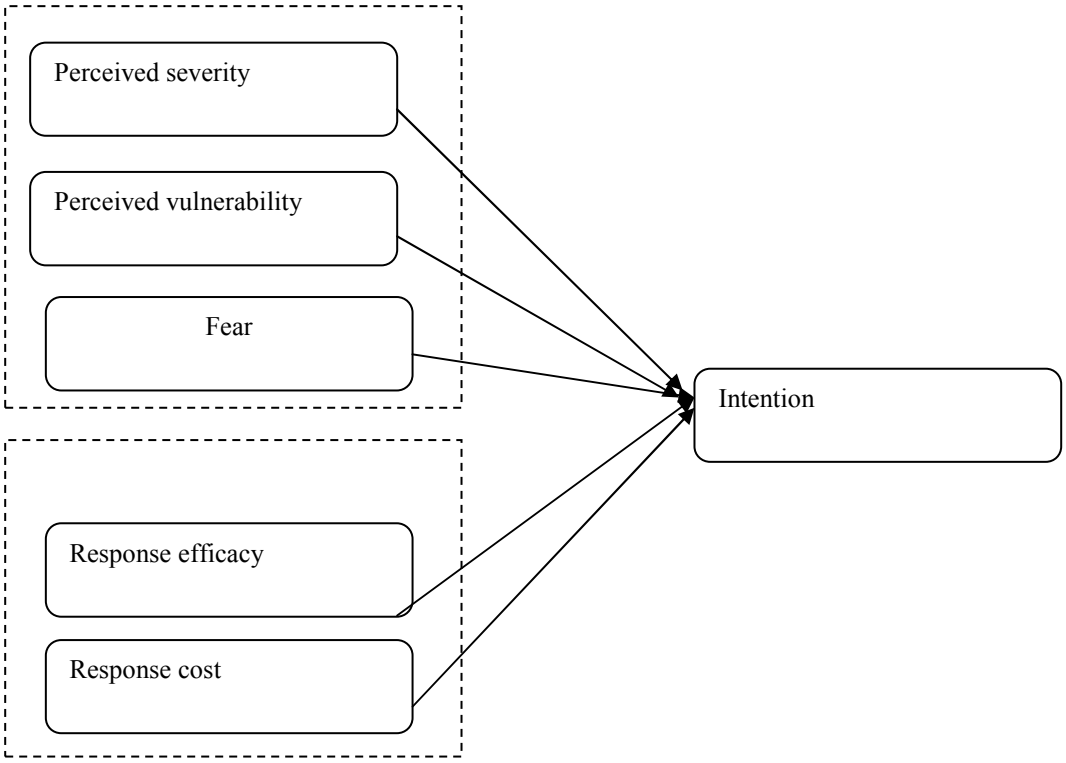

Figure 1: Theoretical Model

Perceived severity

Perceived severity assess how severe a person believes a threat will be to his or her life. On the internet, passwords provide protection to company intranet accounts, bank accounts, social networking accounts, emails and many others. Breach of passwords can cause personal data exposure. The content of emails, personal journals, photos and documents can be exposed to a hacker or public. The exposure of accounting data can even lead to financial losses or identity theft. If the password of the company network was stolen, the company may lose its sensitive and confidential data. Using protection motivation theory, researchers show that perceived severity is significantly related to enabling security measures of a home wireless network (Woon, Tan and Low, 2005).

H1: Perceived severity is positively related to the intention of implementing online password protection

Perceived vulnerability

Perceived vulnerability concerns the susceptibility a person is to the threat. Passwords are very vulnerable to hackers' attack. For example, hackers can use dictionary-based attack, a technique of using program to guess a password by searching possible combinations including common words, slangs and popular phrases. Since computer users tend to choose poor passwords, dictionary-based attack is very efficient. (Campbell, et al., 2007) Passwords can also be guessed after learning an individual's personal facts such as birthday, spouse or parterre's name or pet's name. Another way of compromising passwords is to look over a sticky note or shoulder surfing when someone is typing the password. However, researchers find that people perceive small likelihood of being targeted personally. They believe that people with important information or people who have annoyed the attackers should be concerned (Weirich and Sasse, 2002).

H2: Perceived vulnerability is positively related to the intention of implementing online password protection

Fear arousal

Fear arousal refers to the extent of fear that is triggered by the threat. Fear is an emotional response to threats that can cause change in attitude or behavioral intention (Latour and Rotfeld, 1997). While perceived severity and vulnerability are

cognition-focused, fear is emotion-focused. Studies show that increases in fear are consistently associated with increases in complying with the recommended action (Sutton, 1982: Milne, Sheeran and Orbell, 2000). If online users are very nervous about the prospect of having passwords guessed or cracked by others, they may be more likely to spend more efforts in safeguarding and updating their passwords.

H3: Fear arousal is positively related to the intention of implementing online password protection

Response cost

Response cost measures the perceived costs (e.g. time, money, effort) that a person has to pay in taking the protective behavior. In this study, response cost refers to the time and efforts spent in creating strong passwords and updating them. Most people have gone through the frustration of forgetting passwords and trying to retrieve them. Creating strong passwords and updating them regularly adds more inconvenience. In addition, a wide variety of online accounts also makes the response costs higher. People often reuse their passwords for multiple accounts to minimize the cognitive cost of using the strong passwords.

H4: Response cost is negatively related to the intention of implementing online password protection

Response efficacy

Response efficacy evaluates how effective the recommended coping response in reducing the threat. In order to implement protective behavior, people should be confident that the protective behavior is effective in protecting themselves against the threat. A study investigating cracking time of passwords showed that the majority of passwords that were cracked in less than a minute were all alphabetical characteristics only. All passwords with special characters took at least an hour to crack (Cazier and Medlin, 2006). This shows that strong passwords can protect the online accounts better. In addition to using strong passwords, regular passwords update also help to protect online accounts from malicious hackers. People will be more involved in online passwords protection behavior if they are certain that the extra efforts they invest in making passwords secure are worthwhile.

H5: Response efficacy is positively related to the intention of implementing online password protection.

METHODOLOGY

Data were gathered using an online survey from 182 students in three universities from southern United States. The majority of the students are undergraduate students majored in business. Among the students, 86 of them are males and 97 of them are females. On average, they have about 10.58 years of Internet experience. Regarding the number passwords they use online, 43 of them (23.5%) have 0-5 online passwords, 86 (47%) of them have 6-10 passwords, 38 (20.8%) of them have 10-15 passwords and 15 of have more than 16 passwords (8.7%).

At the beginning of the survey, the following definition of a strong password was provided to the respondents. The definition is adapted from guidelines of Microsoft for strong passwords.

" A password is strong if 1) it is at least seven characters long; 2) it contains characters from letters, numerals and symbols;3) is significantly different from prior passwords; 4) does not contain your name or user name; 5) not a common word or name; 6) have at least one symbol character in the second through sixth positions."

Items used to measure independent variables are listed in the Appendix. All items are developed based on existing scales and are measured on a 5 point Likert Scale. The dependent variable Intention is measured by three items: "I will update my passwords frequently", "I will use strong passwords", and "I will use unique passwords for different online accounts".

Principle component factor analysis using a Varimax rotation was used to assess the dimensionality of the items measuring the independent variables. The criteria of an eigenvalue of at least one was used to assess the number of factors to extract, and the dimensionality of each of the factors extracted was assessed by examining factor loadings (Hair et al.1998). Items with a factor loading of greater than 0.5 on the factor with which they are hypothesized to load were considered adequate indicators of the factors (Hair et al.1998). Items that had factor loadings of 0.3 or greater with another factor were considered to have cross-loaded, and thus were not unique indictors of a given factor. In the latter case, the item would be dropped as the measure was not considered to be unidimensional. For this set of data, the factor analysis yielded five distinct factors based on the Eigenvalue >= 1.0 criteria. The total variance explained by the model is 74.16%.

The second aspect of construct validity assessed is reliability of the measures. One of the most commonly used indicators of reliability is internal consistency, which assesses how consistently individuals respond to items within a scale (Cronbach 1951). Cronbach's alpha is often used to assess the internal consistency of a multi-item measurement scale. Cronbach's

alphas for all fiver factors extracted are above 0.70, which indicates the measures are internally consistent. Table 1 shows the factor analysis results along with the Cronbach's alpha and factor means and standard deviations.

	Severity	Fear	Response Efficacy	Vulnerability	Response Cost
Severity3	**0.952**	0.129	0.032	0.082	-0.005
Severity1	**0.943**	0.182	0.043	0.054	-0.046
Severity2	**0.919**	0.191	0.033	0.092	-0.013
Fear3	0.143	**0.930**	0.094	0.128	0.027
Fear2	0.118	**0.929**	0.063	0.097	0.035
Fear1	0.233	**0.830**	0.121	0.059	0.136
ResponseEfficacy3	-0.018	0.040	**0.912**	0.044	0.001
ResponseEfficacy2	0.019	0.104	**0.887**	0.062	-0.037
ResponseEfficacy1	0.089	0.094	**0.781**	0.001	0.054
Vulnerability3	0.062	0.113	-0.018	**0.816**	0.009
Vulnerability2	0.063	-0.009	0.128	**0.797**	0.063
Vulnerability1	0.065	0.143	-0.010	**0.763**	0.169
ResponseCost2	0.114	-0.045	-0.027	0.037	**0.795**
ResponseCost1	0.046	0.125	0.082	0.219	**0.722**
ResponseCost3	-0.222	0.076	-0.022	-0.004	**0.494**
Cronbach's Alpha	0.917	0.838	0.959	0.728	0.701
Variance Explained	27.12%	14.88%	13.16%	10.89%	8.12%

Table 1: Factor Analysis

RESULTS

Ordinary least squares (OLS) regression was conducted to test the hypotheses. Intention is used as the dependent variable with the five PMT variables as independent variables. The overall model is significant (F= 9.06 and p <0.001). The Adjusted R square is 18.2%. Table 2 shows the results of the regression. Among the five variables, fear, response cost and response efficacy are significantly related to intention. Therefore, H3a, H4a and H5a are supported. Perceived severity and vulnerability are not significant predictors. Hypotheses H1a and H2a are rejected. Table 2 depicts the regression results.

Dependent variable: Intention			
Variables	**Standardized Beta**	**t-value**	**p-value**
Severity	0.03	0.41	0.68
Vulnerability	0.085	1.227	0.22
Fear	0.276	3.735	0.000
Response cost	-0.145	-2.042	0.043
Response efficacy	0.294	4.306	0.000

Table 2: Regression Results

DISCUSSION

Using Protection Motivation Theory, the study investigates the variables affecting computer users' password protection intention and behavior using multiple regression technique. Although both models are significant, the theory is much better in predicting password intention than behavior by explaining more variance of the independent variables. Among the predicting variables of PMT, perceived severity is not related to password protection intention. Evidence for the effects of severity on intentions in previous PMT research has been inconsistent. Researchers have shown that perceived severity is related to intention of implementing information security measures (Workman et al., 2008) and enabling wireless security features (Woon et al., 2005). In our study, perceived severity is not associated with password protection intention. Online users who perceive a severe consequence of password breaches do not necessarily intend to take more efforts to protect their passwords.

Neither is perceived vulnerability associated with password protection intention. According to PMT, the higher probability a user perceives a threat, the more likely he or she will intend to undertake necessary measures. For example, perceived vulnerability is an important predictor of the intention to adopt virus protection measures (Lee, Larose and Rifon, 2008). However, other research also shows non-significant relationship between perceived vulnerability and behavior intention (Murgraff, White and Phillips, 1999).

One possible explanation that the perceived vulnerability and perceived severity are not related to behavior intention was offered by Boer and Seydel (1996). According to them, the threat appraisals play a major role in preventive behavior adoption intention only if the subjects learn about a new and previously unknown threat. In our study, the threats of password breaches are commonly known by the subjects. The severity and vulnerability of the threats are not salient for them so they are not motivated to change their behavior.

We find that fear arousal is positively related to password protection intention. When computer users are scared of the consequences of password breaches, they will take measures to reduce the fear. Compared to perceived severity and vulnerability which are cognition focused, fear, as an emotional response, is a more effective weapon. IS researchers have examined how fear influence the persuasiveness of IT security communication (Xu et al., 2007). Getting computer users emotionally nervous about their information security is helpful in motivating them to comply with security policy, including using strong passwords and updating them often.

The study finds that response cost has a significant negative relationship with password protection intention. In this study, the response cost is measured by difficulty of remembering passwords, which is the major weakness of passwords confirmed by numerous studies. We find that response cost serves as a major deterrent of motivation of protecting passwords. Nowadays computer users have many accounts that need passwords, however, users can only be expected to use four or five passwords effectively (Adams and Sasse, 1999). Therefore, users will inevitably have a huge mental burden if they use strong passwords practice.

Response efficacy has a positive significant relationship with passwords protection intention. This shows that the subjects who believe that the measures taken to protection passwords are effective are more motivated to implement them. Users who believe that their online accounts are vulnerable no matter what passwords they use are less motivated to invest effort and time to use strong password practice.

CONTRIBUTIONS AND CONCLUSIONS

The study presents an empirical examination of computer users' motivations for online password protection intention. While multiple papers have addressed password security, our paper uses a sound theoretical model to examine the behavioral intentions of strong password usage. The security level of the password mechanism largely depends on users' willingness to make efforts to behave in accordance with strong password policies. However, they have to be persuaded to do so. The Protection Motivation Theory posits that people engage in two processes when considering protective behavior: the threat-appraisal process and the coping-appraisal process. After online users evaluate the seriousness of the threat, as well as consider the cost and value of coping strategies, they will make a rational choice on if the protective behavior should be adopted. In our case, the coping-appraisal process plays a major role in online users' intention of implementing good password practice.

The study also presents interesting results for the security professionals. One of the most significant variables that deter users to adopt good password practice is response cost, in this study, the difficulty of remembering the passwords. Since passwords mostly only serve as a mechanism to help users access the main tasks, passwords add extra cognitive load to the users. Therefore passwords are usually chosen on the spot and familiar passwords, short passwords and old passwords are often chosen just for the ease of late retrieval. Unfortunately this is the human cognitive limitation and is hard to conquer. Different

Many researchers have proposed new password mechanism to help to reduce the response cost and improve the quality of passwords. Yan, Blackwell, Anderson and Grant (2004) recommend the use of mnemonic phrases, where the first letters of

each word in a phrase is used as a password. Carstens, Malone and Bell (2006) suggest using passwords consisting of meaningful chunks to improve password recall. Another type of passwords, graphical password, is gaining popularity due to people's superior memory for pictures over texts (Dhamija and Perrig, 2000). Online users need to be educated and instructed to use the new mechanism for their passwords.

The paper also suggests that fear appeal should be emphasized in the communication message for motivating strong password usages. The strong the fear appeal, the greater the intention to adopt good password practice. For example, the message could elaborate on the negative consequence of failure to follow good password practice. Vivid information such as stories and pictures could be used so the contents of the message can be emotionally close to the audience.

REFERENCES

1. Adams, A., and Sasse, M.S. (1999). "Users are not the enemy," Communications of the ACM, 42(12), 41-46.
2. Andrews, L.W., (2000). "Passwords reveal your personality," Psychology today. Accessed from http://www.psychologytoday.com/articles/pto-20020101-000006.html on Feb 17, 2009.
3. Boer, H., and Seydel, E. (1996). "Protection motivation theory," In: M. Conner and P, Norman (Eds), Predicting Health Behavior (95-120). Open University Press.
4. Bryant, K., and Campbell, J. (2006) "User behaviors associated with password security and management," Australian Journal of Information Systems, 14(1), 81-100.
5. Carsten, D.S., Malone, l., and Bell, P. (2006). "Applying chunking theory in organizational human factors password guidelines," Journal of Information, Information Technology, and Organization, 1, 97-114.
6. Carsten, D.S., McCauley-Bell, R.P., and DeMara, R.F. (2004). "Evaluation of the human impact of password authentication practices on information security," Information Science Journal, 7, 67-85.
7. Campell, J., Kleeman, D., and Ma, W. (2007). "The good and not so good of enforcing password composition rules", *Information Systems Security* (16:1), 2-8.
8. Cazier, J.A., and Medlin, B.D. (2006) "Password security: an empirical investigation into E-commerce passwords and their crack time," In*formation Systems Security* 15 (6), 45-55.
9. Cronbach, L. J. (1951) "Coefficient Alpha and the Internal Structure of Tests," *Psychometrika* (16), pp. 297-334.
10. Dhamija, R., and Perrig, A. "Déjà vu: a user study using images for authentication," in Proceedings of 9th USENIX Security Symposium, Denver, Colorado, 45-58.
11. Fiske, S., and Taylor, S. (1984). *Social cognition*. Reading, MA: Addison-Wesley.
12. Florêncio, D., and Herley, C. (2007) "A large-scale study of web password habits," Proceeding of WWW 2007, May 8-12, Banff, Alberta, Canada.
13. Floyd, D.L., Prentice-Dunn, S., and Rogers, R.W. (2000) "A meta analysis of research on protection motivation theory," *Journal of Applied Social Psychology*, 30, 407-429.
14. Gaw, S., and Felten, E.W. (2006). "Password management strategies for online accounts," Proceedings of the second symposium on usable privacy and security, Pittsburg, Pennsylvania, 44- 55.
15. Hair, J.F., Anderson, R.L., Tatham, R., and Black, W. *Multivariate Data Analysis*, 5th edition, Prentice Hall. New York, 1998.
16. Ives, B., Walsh, K.R., and Schneider, H. (2004) "The domino effect of password reuse," Communications of the ACM, 47(4), 75-78.
17. LaTour, M.S., and Rotfeld, H. J. (1997). "There are threats and (maybe) fear-caused arousal: theory and confusions of appeals to fear and fear arousal itself," Journal of Advertising. 26, 45-59.
18. Lee, D., Larose, R., and Rifon, N. (2008). "Keeping our network safe: a model of online protection behavior," Behavior and Information Technology, 27, 445-454.

19. Miller, G.A. (1956). "The magical number seven, plus or minus two: some limits on our capacity for processing information," Psychological Review, 63, 81-97.
20. Milnes, S., Orbell, S., and Sheeran, P. (2002). "Combining motivational and volitional interventions to promote exercise participation: protection motivation theory and implementation intentions," British Journal of Health Psychology, 7, 163-184.
21. Murgraff, V., White, D., and Phillips, K. (1999). An application of protection motivation theory to riskier single-occasion drinking," Psychology and Health, 14, 339-350.
22. Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change," Journal of Psychology, 91, 277-287.
23. Sutton, S. R. (1982). Fear-arousing communications: a critical examination of theory and research. In J.R. Eiser (Ed.), Social psychology and behavioral medicine (303-337). London: Wiley.
24. Tamil, E.M., Othman, A.H., Abidin, S.A.Z., Idris, M.Y.I., and Zakaria, O. (2007), "Password practices: a study on attitude towards password usage among undergraduate students in Klang Valley, Malaysia," Journal of the Advancement of Science & Arts, 3, 37-42.
25. Weirich, D., and Sasse, M.A. (2001). "Pretty good persuasion: a first step towards effective password security in the real world," Proceedings of the 2001 workshop on New **security** paradigms
26. Woon, I.M.Y., Tan, G.W., and Low, R.T. (2005) "A protection motivation theory approach to home wireless security". Proceedings of the 26th International Conference on Information Systems, 367-380.
27. Workman, M., Bommer, W.H., and Straub, D (2008). "Security lapses and the omission of information security measures: a threat control model and empirical test," Computers in Human Beahvior, 24, 2799-2816.
28. Xu, H.**,** Rosson, M. B., and Carroll, J.M., "Increasing the Persuasiveness of IT Security Communication: Effects of Fear Appeals and Self-View," Workshop on Usable IT Security Management, Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA, July 2007
29. Yan, J., Blackwell, A., Anderson, R., and Grant, A. (2004) "Password memorability and security: empirical results," IEEE Security & Privacy, 25-31
30. Zviran, M., and Haga, W.J. (1999). "Passwords security: an empirical study," Journal of Management Information Systems, 15(4), 161-185.

Appendix: Constructs operationalization

Constructs	Items	Source
Perceived severity	How severe do you think the consequence will be if 1. Someone guessed your passwords 2. Someone cracked your passwords 3. Someone obtained your passwords (Ranging from "not severe at all" to "very severe")	Adapted from Plotnikoff and H igginbothanm (2002)
Perceived vulnerability	What are your chances of 1. Someone guessed your passwords? 2. Someone cracked your passwords? 3. Someone obtained your passwords? (Ranging from "Very Unlikely" to "Very Likely")	Adapted from Aspinwall et al., 1991)
Fear	1. The thought of having someone guess my passwords makes me nervous. 2. The thought of having someone crack my passwords makes me nervous. 3. The thought of having someone obtain my passwords makes me nervous. (Ranging from "Strongly Disagree" to "Strongly Agree")	Adapted from Milne et al. (2002)
Response cost	1. If I use strong passwords, it will be difficult for me to remember. 2. If I update my passwords often, it will be difficult for me to remember. 3. If I use unique password on each account, it will be difficult for me to remember. (Ranging from "Strongly Disagree" to "Strongly Agree")	Adapted from Woon et al., (2005)
Response efficacy	I can protect my online accounts better 1. If I use strong passwords 2. If I update my passwords often 3. If I use unique passwords for each online accounts. (Ranging from "Strongly Disagree" to "Strongly Agree")	Adapted from Maddux & Rogers (1983)